Remotely Piloted Aerial System of Systems Survivability:

A Defense-In-Depth Approach

by

E. Lincoln Bonner, III, Major, USAF

Table of Contents

Abstract

Remotely piloted aerial systems (RPAS) are systems of systems. The Department of Defense has identified RPAS to take on dull, dirty, or dangerous combat missions. Political advantages with respect to lowering the threshold for the use of in terms of potential casualties, and military advantages, encourage rapid RPAS deployment. The explosion in RPAS interoperability development has outpaced system level survivability development, resulting in a vulnerable RPAS communication architecture. These vulnerabilities have strategic character, meaning that capabilities designed to attack these weaknesses create strategic, operational, and tactical effects. Obviously, potential enemies could turn weapons designed target these RPAS weaknesses against high value targets creating a deterrent effect. As RPAS combat capabilities begin to supplant manned systems, this deterrence strategy becomes doubly advantageous because the threat not only influences American cost-benefit calculus, but also the United States' ability to respond militarily should the threat be carried out, weakening America's deterrent posture. Fortunately, the Integrated Tactical Warning and Attack Assessment (ITW/AA) system overcame the challenges of protecting RPAS system level weaknesses. The ITW/AA solves these problems by employing a defense-in-depth approach with hardened, redundant communication links and nodes, coupled with a robust systems engineering structure to ensure interoperability without sacrificing survivability. The RPAS community can benefit from adopting an approach to survivability similar the ITW/AA's, which would result less combat RPAS system level vulnerability in the future. It follows that the corresponding military flexibility that would be retained following a strategic assault, which coincidentally targets RPAS system level weaknesses, maintains or improves the United States' military deterrent.

Introduction

As technology rapidly evolves, new capabilities will be realized, but new vulnerabilities will emerge, and some formerly concealed vulnerabilities will be exposed. American armed forces have quickly integrated unmanned systems and unmanned aerial vehicles (UAVs) in particular, into military operations. As technology progresses, the United States (US) military will find UAVs more indispensable in the future.

While convenient to conceptualize UAVs as analogous to manned aircraft, the potential to think of UAVs as autonomous aircraft exists. This potential has led some to prefer the term remotely piloted aircraft (RPAs) rather than the familiar UAV in order to make it explicit that these vehicles aircraft still require pilots, albeit not located in the aircraft. RPA system operators control the aircraft from ground control stations, typically located beyond line-of-sight (BLOS) of the unmanned aircraft. Still the moniker RPV lacks clarity because it fails to acknowledge explicitly that an RPV is a system of systems, consisting not only of the crew in the ground control station and the unmanned aircraft, but also the communication links and nodes between the two. For this reason, the author prefers to refer to UAVs by the term remotely piloted aerial systems (RPAS) in an attempt to capture the complete nature of these systems; they are systems of systems comprised of an unmanned aircraft, piloted by a human crew from beyond line-of-sight, using satellite communication links.

As a system of systems, operators and acquirers should necessarily think of RPAS vulnerabilities in terms of not just the piece at the point of the spear, the unmanned aircraft, the UAV itself, but of the ground control station system and the satellite communications systems weak points too. The integrated tactical warning and attack assessment system (ITW/AA) shares

similar weaknesses with RPAS. The ITW/AA too, composes itself of control stations, the Joint Space Operations Center and Cheyenne Mountain Operations Center; unmanned craft, satellites; and the BLOS communications link needed to control ITW/AA elements worldwide. Unlike RPAS, engineers specifically designed the ITW/AA to account for vulnerabilities across the system of systems, thus solidifying potential chinks in ITW/AA armor while performing its mission to provide attack warning and indications data to the National Command Authority.[1]

When RPAS considering vulnerabilities from a system of systems perspective, particularly soft spots related to the ground control station and the BLOS communication link, realizations of strategic import emerge. Attacking RPAS vulnerabilities requires capabilities that can have effects at the tactical, operational, and strategic levels, to the point that US sovereign options could be limited through an asset hostage deterrence strategy.[2] An adversary achieves deterrence when his opponent fears the consequences of an action to such an extent that he chooses a different course other than the one originally contemplated.[3] An asset hostage deterrence strategy is one in which an objective is achievable, but other assets exceeding the value of the objective are at risk.[4] While American adversaries cannot match the United States' conventional military power, rivals can seek to restrict US freedom of action by holding high-value assets at risk.[5, 6] The fast-paced development and operationalization of RPAS have caused these systems to be fielded with weaknesses that when targeted, reveal vulnerable, high value assets which can be held hostage to America's strategic disadvantage. Adopting an architecture and systems engineering approach for RPAS similar to what the ITW/AA uses, reduces the military utility of developing, and thus an opponent's incentive to develop, weapons to attack these weaknesses.

The following case study compares RPAS system architecture to ITW/AA system architecture. This comparison reveals common vulnerabilities of the two system architectures and discusses the applicability of the ITW/AA approach to shielding these RPAS weaknesses. ITW/AA vulnerabilities are strategic in nature, and attacks in the past on these susceptible points were most likely to be encountered in the context of nuclear war. The appearance of these weaknesses in RPAS, and the rapid spread of RPAS into combat missions will make these vulnerabilities consequential in conventional conflicts at the theater level, a context in which these vulnerabilities could largely be ignored in the past. As opponents develop capabilities to strike at these system level RPAS vulnerabilities, they will gain the power to create effects at the operational level and at the strategic level, which could be used during hostilities, as well as to deter American action in the first place. In the end, this study asserts that RPAS could shield themselves from attack on these weak points by adopting a survivability and systems engineering approach similar to that of the ITW/AA.

Background

Political and operational incentives for RPAS to take on more roles in US warfighting operations exist.[7] The perceived low domestic political cost of using air power (i.e. OPERATION DENY FLIGHT and OPERATION ALLIED FORCE), with the added advantage of not putting personnel at risk is one driving factor. The low political and human cost potential strengthens the national incentive to pursue RPAS. Not putting lives at risk lowers the bar for public support to initiate military action, because potential casualties are a strong factor affecting public opinion in the decision process to use military force.[8] RPAS use can remove the discussion of casualties from the debate entirely, while offering more flexibility than missile

strikes. The Department of Defense (DOD) *Unmanned Systems Roadmap 2007-2032* delineates the operational incentives to use RPAS. This document states that RPAS are best suited towards missions characterized as dull, dirty, or dangerous.[9] The roadmap cites OPERATION ENDURING FREEDOM (OEF), long duration MQ-1 Predator intelligence, surveillance, and reconnaissance (ISR) missions, and long duration B-2 missions originating in the Continental United States (CONUS), as dull.[10] The roadmap and its predecessors identify missions like suppression of enemy air defenses (SEAD), electronic attack (EA), and deep strike, currently performed by manned aircraft like F-16CJs, EA-6Bs, and B-2s, in the dangerous category.[11, 12, 13]

To further illustrate the point, MQ-1 Predator and MQ-9 Reaper orbits in US Central Command's area of operations rose from 11 in 2007 to 33 in 2009.[14] Even the current Secretary of Defense, Robert Gates, believes the F-35 will be the last manned fighter.[15] Given the impetus and stated vision to increase RPAS US military roles and missions, logic leads to the conclusion that potential opponents will likely seek to counter RPAS where they are most vulnerable.[16]

RPAS and the ITW/AA are similar in that both are systems of systems, consisting of command and execution nodes and the links between them, spanning global ranges, with the bulk of command and control (C2) capability for these systems located in the CONUS. RPAS and the ITW/AA differ, however, in scale, complexity, and robustness due to environmental requirement distinctions: the ITW/AA is designed for survivability in a nuclear environment and RPAS are not.[17] Ironically, the requirement for ITW/AA survivability in a nuclear environment drove its architects to address RPAS system level vulnerabilities long ago. The proliferation of RPAS is part of what is bringing these vulnerabilities, once squarely in the purview of nuclear war planners, to prominence in the conventional warfare realm.

The ITW/AA is a network of numerous geographically separated systems across the globe of varying capability: for example, early warning radars located in the CONUS, Greenland, Alaska, and the United Kingdom, and early warning satellite relay stations make up parts of the ITW/AA.[18] The ITW/AA networks all of these systems, ground and space segments, to execute the warning mission. In contrast, RPAS are generally thought of in the context of a single ground control station (GCS) networked to a single UAV. As RPAS numbers go up and their capabilities increase to control multiple UAVs simultaneously from a single GCS, and for GCSs to control different types of UAVs, RPAS similarities to the ITW/AA will rise. The multiple BLOS communication links between GCSs and UAVs will generate networks of size and scope similar to the ITW/AA. This in essence reflects the approach the entire US military is moving toward, network-centric warfare. The ITW/AA has been engaged in network-centric warfare for decades now. Even so, the analogy in vulnerabilities between the ITW/AA and RPAS does not rely on the assumption that a vast RPAS network exists. Rather, one can view the ITW/AA weakness mitigation strategy in its application to individual sensor nodes--the control segment, a single operational sensor segment, and the link between them--so comparison with the current RPAS architecture, consisting of one control segment, the GCS, and one operational segment, the UAV, and the link between them, is realistic.

Remotely Piloted Aerial System Vulnerability & Protection

Direct Action against the Ground Control Station

To attack any target, it must first be found, then tracked, and lastly struck. The requirement to track a target disappears if it is stationary, shortening the kill chain. The RPAS C2 segment, the GCS, to date largely located at CONUS bases, offers such a static target. The

kill chain shortens more if the target location is public knowledge, much like the general location of RPAS GCSs. The MQ-1 Predator operations out of Creech Air Force Base (AFB), Nevada, for example, have been the subject of several television and radio news reports.[19] Nevada State Highway 95 runs within yards of the Creech AFB's main gate, with much of the surrounding land accessible to the public. Typically, RPAS GCSs are not physically hardened structures, nor are there back-up facilities at a secondary location to pick up operations seamlessly in the event of failure.[20, 21] Lack of redundancy gives operational utility to attacking the GCS for disrupting RPAS operations, and lack of hardening makes such an attack a viable option for a potential adversary. The MQ-1 GCSs, trailers, are relatively "soft" targets that, if located with enough precision, could be attractive to an otherwise overmatched adversary.[22] Given the close proximity to civil aviation airspace, a 9/11 style attack with a piloted aircraft or enemy RPAS as simple as a Cessna 172 light airplane could be extremely effective against MQ-1 GCSs. While MQ-1 GCSs are air transportable, that offers little utility if the primary operating location is public and easily assaulted.[23] The MQ-1 GCS example illustrates the general approach the US military has taken toward deployment of RPAS C2 facilities to date: stationary, lightly hardened facilities at known locations inside CONUS, the homeland. The operational effectiveness of attacking CONUS air bases lessens with the bulk of combat airpower forward deployed during a conflict. As RPAS take on a greater percentage of combat missions, operational incentives to attack the homeland will increase if GCS survivability characteristics remain unchanged. why spend time and effort fielding counter low observable integrated air defenses if crashing a light aircraft into a group of trailers, whose location can be found by an internet search or simply watching CNN, achieves the same operational effect?

Any capacity to attack the American homeland directly, whether actually used against RPAS or not, has the potential for direction towards strategic ends by targeting critical infrastructure. Such a strike could wreak havoc in the American economy and politics in the short term, or over the longer term depending on the scope and depth of the assault. Power substations, ports, and suspension bridges are just a few examples of potential targets with similar characteristics to current RPAS GCSs: stationary, soft, with a known location. The ability to threaten widespread assault, or to carry out carefully selected attacks against civilian targets of the type described above, serves to give the United States pause before taking action in situations presenting less direct threats to American national security. Holding such soft targets at risk can deter America and limit its freedom of action, as well as negate RPAS given its current GCS paradigm.

Like RPAS C2 facilities, much of the ITW/AA's C2 infrastructure is stationary, the location of its facilities public knowledge (i.e. Cheyenne Mountain Complex). The ITW/AA's approach to lessening the vulnerability to direct attack on its C2 nodes is to physically harden the GCSs, and to have back-up and/or mobile GCSs, capable of assuming the C2 functions of the primary GCSs, and/or controlling multiple operational segments of the ITW/AA. The Milstar communication satellite constellation for instance, part of the ITW/AA communication network, uses multiple mobile and fixed GCSs to provide survivable C2 links for the constellation to protect against direct attack on its GCSs.[24] The 4th Space Operations Squadron's primary GCS at Schriever AFB provides robust, hardened Milstar C2.[25] Milstar mobile GCSs increase C2 survivability for this portion of the ITW/AA, because mobile GCS movements, operations, and deployments are generally unpublicized events, if not actually classified. Secret Milstar mobile

GCS movements and operations decrease an opponent's capability to negate the Milstar's C2 segment, correspondingly increasing ITW/AA survivability.

Changing the RPAS C2 paradigm to resemble more closely the ITW/AA's, and the specific example of Milstar, could significantly complicate an adversary's decision calculus regarding the operational feasibility of direct attack on RPAS GCSs. Multiple redundant GCSs, and/or mobile GCSs with unknown or unpredictable combat operating locations, can add significant complexity to an opponent's targeting problem versus the RPAS C2 segment. Developing future GCSs that provide mobility and redundancy, particularly as RPAS combat roles increase, can provide marked increases in RPAS survivability while increasing the cost of fielding capabilities to negate RPAS C2. This result reduces an opponent's incentive to target RPAS GCSs as a military operational tactic.

Jamming

RPAS and ITW/AA link segments are vulnerable to EA at the GCS antenna (downlink jamming), the satellite antenna (uplink jamming), and the communications antenna onboard the UAV (downlink jamming).[26, 27, 28] Two satellite links can affect RPAS performance: communication and navigation links.

While military satellite communication (SATCOM) was originally intended to provide strategic, BLOS communication between fixed military bases, SATCOM has become a necessity in global commerce and conventional military operations at the tactical and operational levels.[29]

Combat RPAS' need for BLOS command links makes SATCOM even more critical at the tactical and operational levels. The RPAS C2 link passes data in two directions: commands from the GCS to the UAV, and state-of-health (SOH) data from the UAV to the GCS. Both data paths

are susceptible to uplink jamming. The SOH data path is the more vulnerable of the two, because one way to defeat uplink jamming is to boost transmitter power, a much easier task from a ground station than from an aircraft where the sole power source is the onboard generator. A 2005 RAND study on UAV support considerations highlighted the reliance on commercial satellites for high data rate, BLOS communication as a consideration for both MQ-1 Predator and RQ-4 Global Hawk RPAS.[30] Commercial communication satellites are susceptible to EA because they are designed to function in a benign environment at minimum cost.[31] Communication satellites are generally in geostationary orbit (GEO), a relatively fixed position that makes them easier to target. The combination of a simple tracking problem and a "soft" target adds to commercial communication satellite vulnerability to uplink jamming. The cost, $30K to $1M, and technical bar to build effective, small, mobile uplink jammers, are relatively low.[32] Given that standard operating procedure for loss of the RPAS C2 link is for the unmanned aircraft to return to base automatically, and that RPAS rely on commercial SATCOM for BLOS operations, uplink jamming EA is an attractive option to negate RPAS.[33] The DOD *2007-2032 Unmanned Systems Roadmap* highlights securing command links to unmanned systems as one of the top two technology challenges in RPAS development and operations, likely because uplink jamming provides such an enticing method to defeat RPAS.[34]

In addition to suppressing RPAS, uplink jamming has the potential to limit theater communications in general, as well as communications at the regional level with negative effects on the military and potentially regional commerce. SATCOM uplink jamming capabilities developed to counter RPAS can therefore produce tactical, operational, and strategic consequences. The ability to employ SATCOM uplink jamming is thus a strategic capability, the

military incentives to which RPAS communications debilities accentuate. Downlink jamming targeting the navigation can create similar strategic effects.

Combat RPAS will likely rely on a navigation link, a satellite link with the Global Positioning System (GPS), for onboard navigation to determine where the UAV is in space. Employing weapons from a moving platform such as a UAV, requires accurate navigation data as a first step; the system cannot accurately predict where a free fall bomb will land if the system does not accurately know the release point. The ability to generate accurate position information onboard the UAV takes on greater criticality because operators must account for the command time delay between the RPAS GCS and UAV at global ranges. This fact probably prohibits "dumb" bomb weapons employment without accurate time, space, and position information (TSPI) onboard the UAV to account for the time difference between the GCS transmitting the release command, and weapon drop from the UAV. It is a reasonable inference that RPAS rely on GPS data for accurate TSPI given that manned aircraft leverage GPS data for similar functions, and the MQ-1, MQ-9, and RQ-4 RPAS all have GPS minimum essential system requirements for takeoff in their operating procedures.[35, 36, 37] The trend toward smaller weapons, like the small diameter bomb (SDB), places greater emphasis on bomb accuracy and precision, increasing the need for exact TSPI from systems like GPS. Although modern inertial navigation systems (INSs) are very good, they do drift and require periodic update to maintain accuracy and precision. The criticality of INS drift grows with mission duration, because INS error is directly proportional to the length of time between position updates; the shorter the time between updates, the smaller the INS error, and the more accurate and precise the TSPI. Adversaries can turn the same simple, cheap SATCOM uplink jamming technology to jamming GPS downlink transmissions with little difficulty. Subsequently, GPS jamming offers a low

cost, effective mechanism to limit combat RPAS mission success by decreasing weapon accuracy, potentially to the extent that the TSPI inaccuracies prohibit weapons release altogether. The proliferation of GPS into everyday life worldwide means that denying its use at the regional level could be vastly disruptive to global commerce. Commercial banking transactions rely on GPS time to execute electronic transactions worldwide and the reduced vertical separation minimums (RVSM) standard being instituted globally to reduce air congestion requires GPS navigation.[38, 39] Disruptions to global networks like air traffic control and banking at the regional level through GPS jamming could have strategic economic impact, as well as operational and tactical military consequences.

The ITW/AA has evolved to deal with the threat of SATCOM jamming and TSPI inaccuracies. The ITW/AA addresses the SATCOM uplink jamming threat by employing defense-in-depth: multiple redundant SATCOM paths, jam resistant SATCOM, and parallel fiber-optic and cable hard line communication links.[40, 41] Similar methods can protect the RPAS links between the GCS and the UAV operational segment. Essentially, the ITW/AA's multiplicity of redundant communication nodes and links makes its communications not only jam resistant, but also attack resistant in general. Developing multiple communication pathways between the GCS and UAV, operating in parallel or rapidly switchable, is a potential solution. For instance, medium earth orbit (MEO), or low earth orbit (LEO) SATCOM constellations, like Iridium, can provide multiple redundancy for C2 links and nodes.[42]

The solution to RPAS TSPI errors generated by GPS jamming also lies in redundancy, having multiple ways to update the INS onboard the UAV. Like RPAS, the ITW/AA must account for TSPI inaccuracies, particularly in the space based missile warning mission. To geolocate a missile launch detected by a GEO missile warning satellite (i.e. a Defense Support

Program satellite), the associated ground station computes the missile launch location using the satellites position as the basis for the calculation. Because the distance between geostationary warning satellites and the earth is large, small discrepancies between GCS predicted satellite position and actual satellite position could lead to significant errors in missile warning data. The ITW/AA relies on ground based radar data uploaded to missile warning GCS processing databases to provide accurate satellite TSPI, known as ephemeris. A similar capability to upload TSPI updates to the UAV from off-board or onboard sensors could mitigate the results of GPS jamming on combat RPAS.

Anti-Satellite Weapons

RPAS SATCOM and GPS C2 links to the UAV are vulnerabilities that enemies can exploit by attacking the link itself using EA, or by attacking the satellite node using anti-satellite (ASAT) weapons. China and Russia have already demonstrated hit-to-kill anti-satellite weapons, but these are of lesser concern because the targeting and missile technology hurdle to develop this type of ASAT capability is relatively high.[43, 44] A less technically challenging ASAT method to target LEO or MEO constellations, such as GPS, is to simply litter the three-dimensional surface occupied by the constellation with space junk.[45, 46] The advantage of this ASAT method is that the capacity to inject significant payloads into orbit is not required, so the necessary missile technology is more attainable, particularly in light of proliferation and advancements in missile technology.[47]

High altitude nuclear detonation (NUDET) poses another ASAT threat.[48, 49] The electromagnetic pulse (EMP) generated by such a blast has the power to cause serious short and long term disruption to satellite systems indiscriminately.[50] For NUDETs between

approximately 100 kilometers (km) and 500 km altitude, LEO and MEO satellites are the most vulnerable, with GEO satellites at risk too, albeit low.[51] NUDETs near GEO altitude present greater risk to GEO satellites, but this requires significantly better missile capability. Although the probability of a high altitude NUDET damaging GEO communication satellites that relay RPAS data between the UAV and GCS is lower, the scenario cannot be ignored because the resultant loss of BLOS C2 links could render combat RPAS useless under current operating architecture. Increased Van Allen Belt radiation could render inoperable unprotected LEO satellites, not negated by the initial EMP, in a matter of days.[52] MEO satellites surviving an initial EMP attack could see their lives end within weeks or months of an assault, also as a consequence of greater Van Allen Belt radiation.[53] Consequently, a high altitude NUDET attack has the capability to destroy and/or substantially degrade the GPS constellation, in MEO, with negative ramifications for RPAS TSPI accuracy, essential for combat RPAS weapons employment.[54]

The strategic implications of high altitude NUDET capability cannot be understated. An attack of this type would disproportionately affect Western nations, as the bulk of the satellites in orbit belong to Western governments and corporations. There is also the impact on regional allied infrastructure to be considered. The 2008 *Report of the Commission to Assess the Threat to the United States from EMP Attack* determined that a high altitude NUDET strike on America would be catastrophic due to its dependence on electronics in the system of systems that make up the country's critical infrastructures.[55] Coincidentally, this type of strike would affect EMP vulnerable RPAS ground stations too. Electronically dependent allies like Japan and Taiwan could anticipate experiencing similar effects from a high altitude NUDET. The costs of such an attack, in terms of resources to reconstitute space systems and electronically dependent

infrastructure, would be staggering, not to mention the second and third order economic effects given that satellite use has become ubiquitous in global commerce.[56] Strategically, operationally, and tactically no doubt exists as to the effects a high altitude NUDET can cause.

Some may argue that such an attack would elevate a situation beyond the scope of conventional, force-on-force conflict, and demand a massive strategic retaliation, implying a nuclear counter-strike.[57] Under this logic, an opponent would not dare detonate a nuclear weapon, even in outer-space, unless planning to engage in nuclear war. In this scenario, systems apart of the nuclear triad, like tactical combat RPAS, need not be designed to survive a NUDET EMP. The threat of massive American nuclear retaliation under these circumstances seems incredible. It is difficult to imagine a scenario in which the US Government would sanction taking tens of thousands of civilian lives by launching a retaliatory nuclear strike in response to a high altitude NUDET that likely resulted in no human casualties and no increase in surface radioactivity. A massive nuclear retaliation would seem to go against the grain of America's just war traditions, particularly the *jus in bello* principles of discrimination and the doctrine of double effect.[58] In light of this just war tradition, a massive conventional reprisal seems the more likely course of action in response to a high altitude NUDET. Given the decision calculus from a US opponent's frame of mind, a handful of nuclear weapons and the threat of a high altitude NUDET is an attractive deterrent option, because an EMP strike is unlikely to spark nuclear retaliation should an antagonist choose to carry it out. Moreover, the EMP strike may yield decisive near-term operational advantages against America's technology dependent, conventional military. Worst of all, the cost to the United States and her allies would be so high that there is a good chance they would not act in the face of an EMP threat, except when their most vital national interests were at risk. US Marine Corps Brigadier General Kenneth

McKenzie's paper, "Revenge of the Melians: Asymmetric Threats and the Next QDR," speaks to this line of reasoning, as well as the potential strategic, operational, and tactical implications of a high altitude NUDET for the United States quite convincingly.[59]

ASAT weapons, conventional or nuclear, potentially impact RPAS operations significantly by breaking the C2 and or navigation links RPAS depend on. The ITW/AA dealt with ASAT threats to its communication system architecture with redundancy and electronic hardening, essentially EMP armor.[60, 61] Electronic hardening prevents propagation of an EMP through electronic systems, protecting critical elements of the ITW/AA, space and ground segments. RPAS can benefit from adopting a communication architecture with redundancy and electronic hardening features similar to the ITW/AA.

System of Systems: Interoperability & Survivability

As RPAS evolve to assume more combat functions, especially in hostile, denied access areas, the overall system level vulnerabilities must be addressed, in addition to the traditional survivability of the UAV itself against conventional air defense weapons. The DOD *Unmanned Systems Roadmap 2007-2032* clearly states: "[a]dressing the survivability of simply the platform only partially addresses the survivability of the total system as the components operate within a collaborative multiplatform environment," and, "[f]uture efforts should concentrate on reducing the total system susceptibility and vulnerability." [62] Of the three roadmaps relating to RPAS development produced since 2000, the 2007 document is the first to acknowledge the system of systems character of RPAS vulnerability.[63, 64] Although the 2007 roadmap acknowledges the system of systems nature of RPAS weaknesses and the impact on survivability, the corresponding connection between survivability and interoperability in a system of systems

environment appears missing. For example, the Unmanned Aerial Systems Planning Task Force (UAS PTF) and the Joint Unmanned Aircraft Systems Center of Excellence (JUAS-COE) both have responsibilities to facilitate systems engineering tasks of interoperability and standardization, but neither systems engineering nor survivability are mentioned in relation to these organizations.[65] The 2007 roadmap and its predecessor documents talk about interoperability and survivability separately.[66, 67, 68] Interoperability receives a whole chapter devoted to it in the 2007 report, while survivability warrants just a few sentences.[69] The separation and lesser emphasis on system level survivability illustrate the lack of balance in the RPAS systems engineering effort, focusing on interoperability without explicit accounting for the effect of interoperability on survivability. The 2007 roadmap fails to account for the fact that survivability and interoperability cannot be divorced when dealing with a system of systems like RPAS, which operate over a network. As the 2007 roadmap states, "Interoperability is achieved by *buying* common components, systems, and software and/or by *building* systems to common standards." [70] These components, systems, software, and standards almost axiomatically affect RPAS survivability. Security, protection, and survivability should be reckoned with, at or near design inception as a primary driver, while concurrently striving for maximum interoperability.

Dr. Vinton Cerf, Google's internet guru and one of the inventors of the internet, said in his remarks at the 2009 Air Force Association Air and Space Conference that had he considered security an important factor in his initial work, the internet protocol (IP) used today would not be the standard.[71] The problem that Dr. Cerf faced was that the world agreed upon and perpetuated his original IP as the standard by the world community before he could finish work on a more secure protocol.[72] The less secure IP rapidly spread into today's world wide web, resulting in

many of the internet security problems faced now, all because interoperability was the focus without due regard for security and protection from the outset.

There appears to be an implicit assumption that C2 links will be available, that the US military will have access to the global information grid. As a result, RPAS vulnerabilities at the system level, related to the communication link between the GCS and UAV, appear disregarded, while interoperability with other platforms remains a focus. The survivability focus for RPAS has been dominated by the manned aircraft survivability paradigm, the shoot down problem, as the 2002 and 2005 roadmap survivability sections discuss.[73, 74] Current RPAS mission profiles to collect ISR data in relatively permissive environments have not required system of systems survivability analysis, but forecasted mission expansion into activities like SEAD for combat RPAS must not ignore these survivability issues. As stated in the introduction, there is no need for an adversary to go through the trouble of trying to shoot down a difficult to target like low-observable UAV, when the enemy can simply direct some jammers at a few fixed points in the sky and get the UAV to turn around and go home. The systems engineering focus on interoperability, without the corresponding emphasis on survivability, may end in combat RPAS fielded with excellent interoperability features open to exploitation, similar to the situation with the World Wide Web.

There is a lack of overarching, comprehensive, systems engineering oversight and responsibility for RPAS that has lead to a focus on interoperability and without due regard to system level survivability. RPAS systems engineering responsibilities fall primarily on two organizations, the UAS PTF and the JUAS-COE. The UAS PTF holds responsibility for guiding RPAS execution and planning under the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD (AT&L)).[75] The JUAS-COE, under US Joint

Forces Command (JFCOM), retains the charter to facilitate common operating standards to improve interoperability.[76] A review of the key DOD directives (DODDs) of interest to these RPAS systems engineering organizations and program managers shows a focus on interoperability.[77] Of the 14 directives, only one addresses system protection, DODD 8500.1 *Information Assurance*, and it focuses on computer protection from cyber attack.[78, 79] Additionally, the 2007 roadmap goes on to describe the activities and results of four RPAS study groups, six RPAS working groups and organizations, and six laboratory organizations within DOD alone, not to mention the myriad of organizations within the Department of Homeland Security, Department of Transportation, Department of the Interior, Department of Commerce, and the National Aeronautics and Space Administration (NASA) working RPAS interoperability issues in some form or fashion.[80] Furthermore, the term "systems engineering," or variations thereof, appears only three times in the text of the 2007 roadmap, a 189 page document.[81] Where the document mentions "systems engineering," it is only in relation to interoperability issues. An essential systems engineering consideration is interoperability, but as the Naval Post-graduate School defines it, "Systems Engineering is an integrated approach to the synthesis of ***entire*** systems." [82] The 2007 roadmap does not seem to acknowledge that systems engineering for a combat system like RPAS, should not only account for interoperability, but all aspects of the system of systems, to include design integrity, survivability, endurability, compatibility, security, performance, and reliability.[83] The description of the two primary RPAS organizations with systems engineering responsibilities, the UAS PTF and JUAS-COE, does not discuss most of these systems engineering terms.[84] The ITW/AA systems engineering organization offers an alternative to the current decentralized and incomplete RPAS systems engineering structure

capable of addressing both interoperability and survivability issues in a system of systems context.

Accurate ITW/AA data informs decisions makers with the information necessary to respond to nuclear attack. Consequently, the ITW/AA, or at least its communications elements, is part of the US nuclear command, control, and communication (C3) system of systems. The nuclear C3 system falls under the purview of a single systems engineer, supporting the Joint Staff J-6, who oversees system design integrity, interoperability, survivability, endurability, compatibility, security, performance, and reliability.[85] Having a single office charged with making recommendations and capturing lessons learned for the critical nuclear C3 system of systems across the range of systems engineering challenges, encompassing all operationally relevant facets of the system, including survivability, provides over watch for the nuclear C3 system of systems, limiting the chance that a key issue will be overlooked. RPAS, could benefit from an office performing a similar function, providing overwatch to ensure that survivability is not unintentionally sacrificed for interoperability.

Recommendations

RPAS vulnerabilities are similar to those of the ITW/AA. As RPAS military use expands, operational incentives for opponents to target these vulnerabilities will increase. The result could be a scenario in which the United States is deterred from acting due to the potential for negative strategic effects, generated by capabilities whose development was spurred, in part, by the desire to negate RPAS. The United States can reduce the military operational and tactical rewards from targeting RPAS system level vulnerabilities. The ITW/AA approach to increasing survivability in recognition of RPAS shared weaknesses is to essentially employ a defense-in-

depth where no single attack, and no single means of attack, can disable the system of systems. RPAS can benefit from a similar defense-in-depth strategy for protection so that no one assault, and no one countermeasure, can disrupt or defeat combat RPAS. Technology investment, systems engineering, and policy recommendations to facilitate implementing a system level, defense-in-depth strategy for RPAS follow.

Technology Investments

Direct Action

Two technology investments are worthwhile to increase RPAS GCS survivability in the face of direct physical attack, emulating the ITW/AA: commonality and hardening. To this end, OUSD (AT&L) should strongly encourage common control, like the US Army's OneSystem common GCS for its RPAS, within each service, if not a joint RPAS GCS system.[86] The 2007 unmanned systems roadmap identifies common control as a technology objective for reasons of efficiency and logistics, but does not cite survivability as a rationale to pursue this goal.[87] The contribution to defense-in-depth that common control provides an RPAS dependent force, warrants making this technology objective a priority. Common control can ensure the ability to rapidly shift UAV C2 to back-up GCSs with minimal impact to operations should a ground station attack occur.

Unlike common control, physical hardening of RPAS GCS does not require any new technology investment, only infrastructure investment. DOD should seek to consolidate RPAS operations in a few, permanent, hardened facilities similar to the space operations centers working out of Schriever AFB's satellite mission control facility. These facilities would not replace the mobile GCSs now in use, but take over as the primary operating location. Mobile

GCSs would be retained to provide greater operational flexibility and survivability, so that no one physical attack, and no single attack operational concept, could destroy the majority of RPAS ground control capabilities in one fell swoop. As part of the RPAS concept of operations, the military should not publicize locations executing active, combat RPAS C2 operations, even to the point of classifying these operations.

Jamming

The ITW/AA foils the uplink jamming threat by using jam resistant SATCOM links and through multiple redundant communication paths, so that disruption of any single path does not disrupt communication for the system. To create a redundant system with similar features for RPAS, the DOD should alter its BLOS communication scheme away from monolithic, geostationary SATCOM, and invest in LEO and near-space communication platforms. This type of BLOS communication architecture reduces uplink jamming effectiveness, because multiple communications platforms will likely be in the UAV field of view so that no single jammer can thwart all communications paths.[88] Additionally, enemies would have to track these moving communication nodes to keep the jammer locked on them and deny UAV communication with the GCS. Geometry can also be used advantageously so that it is possible to choose BLOS platforms within the UAV's LOS, but out of jammer threats' LOS.[89] Lowering the communication platform altitude has the added benefit of reducing the transmitter power required, because received signal strength varies inversely proportional the distance squared. If the satellite and UAV communication packages remain unchanged, jam resistance increases because of the corresponding increase in signal to noise ratio, meaning an enemy will need a more powerful jammer to be effective. Alternatively, the communication payload on both the

UAV and the communication node can be made smaller because they require less power due to closer proximity. The Iridium communication satellite constellation, the Battlefield Airborne Communication Node (BACN), and Open Gateway are representative of the types of communication investments needed to provide multiple redundant RPAS C2 links.[90] As these systems are developed, it is crucial that the high bandwidth RPAS C2, SOH, and sensor data requirements be key performance drivers. Additionally, BACN and similar systems should be installed on as many platforms capable of carrying the communication payload as possible, for instance on tankers and other airlift assets. One can envision an air communication bridge of airlift assets providing secure redundant BLOS C2 for RPAS while simultaneously sustaining operations in theater. Ideally, these assets would form an air and space communication network that would function similar to the internet, where different communication payloads would optimally route message traffic based on a destination address alone.

To facilitate this ultimate vision for battlefield communication, a key enabling technology is necessary, delay tolerant networking (DTN). Currently, internet communication protocols require a continuous link, something that the fog and friction of a battlefield environment makes unlikely.[91] DTN, pursued by the Defense Advanced Research Projects Agency and NASA, makes use of store-and-forward techniques to compensate for intermittent connectivity.[92, 93] DTN, combined with a multiplicity of airborne and space communication platforms, has the potential to greatly increase RPAS C2 link protection in a jamming environment.

Just as redundancy is an effective SATCOM uplink jamming countermeasure, TSPI source redundancy is a useful GPS, downlink jamming countermeasure. RPAS need a way to update UAV onboard TSPI in a GPS denied environment, similar to the ITW/AA's capability to upload satellite ephemeris to its ground stations. Investments should be made such that the GCS

can perform manual updates to the UAVs onboard navigation system using own-ship or off-board sensors. Previously discussed investments to improve C2 link redundancy will improve the ability to perform these updates in a jamming environment. Another investment priority in the near-term is autonomy for the UAV to perform position fix updates without GCS control. In the event of lost C2 and GPS, the UAV may need to continue its mission and still be able to accurately employ weapons. The ability for the UAV to take a navigation fix with own-ship sensors and update its INS is a worthwhile investment in autonomy that is likely reachable in the near-term.

ASAT

Ironically, shifting RPAS communication systems to LEO and airborne platforms for better jamming protection, would make these communication nodes more susceptible to attack from surface-to-air missiles and/or ASATs. Fortunately, the redundancy that raises RPAS EA protection in this architecture by increasing the number of communication nodes that a foe must render inoperable applies to kinetic attacks too. Redundancy alone though does not protect against the EMP threat presented by a high-altitude NUDET. Electronic hardening of a subset of these communication nodes is also necessary just as it is in the ITW/AA. Investment in boost phase ballistic missile defense and EMP hardening verification capabilities at the sub-system, or preferably at the system level, is also necessary to create defense-in-depth against a high altitude NUDET EMP.

The current US missile defense system consists of three layers, boost, mid-course, and terminal defense weapons, designed to protect the United States and its allies from a weapons of mass destruction, ballistic missile strike from a rogue nation armed with a small number of

munitions. Of these three layers, only boost phase defenses are effective against preventing an EMP attack by high altitude NUDET. To execute this type of assault, an enemy missile need only reach detonation altitude; range is a secondary consideration. A nation could even launch an effective strike by detonating a weapon above her territory.[94] Even intermediate range missiles like the Al Hussein burnout at 150 km altitude, well above the effective altitude needed to cause EMP damage.[95] The other two layers of missile defense are useless when confronted with this operational concept. Investment in boost phase missile defense technology, particularly speed-of-light weapons like the Airborne Laser, is necessary to counter this threat because the time from missile launch to detonation at 100 km altitude is about 100 seconds, the time in which to execute the entire missile defense kill chain against a high altitude NUDET attack.[96]

In sync with the defense-in-depth theme of RPAS technology investment recommendations, electronic hardening of a key subset of RPAS systems should be performed, to include the GCS, UAV, and communication nodes, such that combat RPAS operations can still be executed following an EMP attack. There is a need to harden critical civilian infrastructure to withstand a NUDET EMP attack also.[97] The techniques of EMP hardening are well understood, but live fire testing validation of these protections is no longer possible. In the past, this validation testing was performed at the system or subsystem level during nuclear weapons tests. Since signing the Comprehensive Test Ban (CTB) Treaty, the United States no longer does these tests. The American solution to the validation problem was to build a massive x-ray pulse machine, called DECADE, to simulate the prompt radiation EMP effects of a nuclear blast. When the Cold War ended, the government eventually terminated the project before completion because only one customer with a requirement for EMP protection validation testing remained, the Missile Defense Agency, so the facility was not cost effective. Current EMP

testing facilities are only able to perform validation at the component level. Validation of system and subsystem EMP protection relies on design verification, computer modeling and simulation, and careful quality control. The problem with this methodology is that EMP weaknesses often result from interfaces between components or subsystems. To harden RPAS and other military and national infrastructure critical systems, the nation should invest in the capability to perform prompt radiation testing, at a minimum on electronic subsystems if not whole weapon systems.

Systems Engineering

Unlike the ITW/AA communications backbone, no single office or individual is responsible for RPAS systems engineering in total. As a result, there is an apparent secondary prioritization of survivability relative to interoperability in the RPAS system of systems context. The results of such unbalanced focus has historical precedent: the vast security vulnerabilities of today's world wide web can be attributed to a rush toward interconnectivity and interoperability unbalanced by protection concerns, to the detriment of cyber security today. OUSD (AT&L) or the Chairman of the Joint Chiefs of Staff (CJCS) should designate an RPAS Systems Engineer, with responsibilities similar to those held by the Nuclear C3 Systems Engineer outlined in CJCS Instruction 5119.01C. These responsibilities include making recommendations to the Joint Staff on interoperability, endurability, reliability, compatibility, security, performance, and survivability of the nuclear C3 system.[98] The RPAS Systems Engineer should have similar responsibility to the Joint Staff for the RPAS family of systems. The RPAS Systems Engineer should not have the authority to impose policy or standards, but should be responsible for making recommendations that balance all of the military performance requirements across the range of RPAS capabilities in the system of systems, network-centric-warfare environment. Like

the Nuclear C3 Systems Engineer, RPAS Systems Engineering duties should encompass acquisition functions as well as training, readiness, and exercise evaluation functions.[99] This scope of responsibilities improves the opportunity to create synergy between technology development, operational lessons learned, and tactics, techniques, and procedures. Given the inclusion of training, evaluation, and readiness functions, it is more appropriate that the RPAS Systems Engineer fall under the Joint Staff rather than OUSD (AT&L). Of the two standing RPAS systems engineering organization, JFCOM's JUAS-COE is the better candidate to take on RPAS Systems Engineer duties. The Joint Staff has already charged this organization with RPAS Systems Engineer duties within the subset of interoperability, operational lessons learned, exercise evaluation, and training.[100] Therefore, it is recommended the UAS PTF be folded into the JUAS-COE, the director of the JUAS-COE be designated the RPAS Systems Engineer, and the JUAS-COE's charter be expanded to include the relevant systems engineer responsibilities bestowed upon the Nuclear C3 Systems Engineer as described in CJCSI 5119.01C.

Policy

The DOD should commit to an RPAS survivability and protection policy that relies on defense-in-depth, redundancy and layers, to ensure that as combat RPAS evolve to take on more missions that are dangerous, they are able to function across the spectrum of conflict, even in the face of potential enemy countermeasures. This is a crucial policy choice, because the RPAS countermeasures described in this study can produce tactical, operational, and strategic level effects. A defense-in-depth approach for the RPAS system of systems architecture can mitigate the tactical and operational level consequences of these enemy threats reducing their deterrence value. This means that an adversary who chose to employ RPAS countermeasure weapons

against strategic targets would not gain a significant military advantage over RPAS, or ostensibly over other US conventional military capabilities, to defend against the reprisal that would be sure to come. The loss of substantial operational and tactical advantage by employing RPAS countermeasures against strategic targets reduces the likelihood an opponent could retain whatever gains he sought, even in the short term. RPAS defense-in-depth facilitates a US capability take back these gains producing a deterrent effect, reducing the chance that an enemy may choose to act on a threat.[101]

Conclusion

RPAS are systems of systems whose technical and political advantages in the dull, dirty, and dangerous missions make it likely they will largely supplant manned aircraft for these combat roles in the future. The current RPAS systems architecture, particularly the BLOS C2 link and GPS navigation link, is vulnerable to attack. The RPAS GCS is susceptible to physical attack. The SATCOM nodes are vulnerable to electronic attack, kinetic anti-satellite weapons, and nuclear EMP attack. The ITW/AA system of systems shares these weaknesses, because these chinks are largely the soft spots of any generic SATCOM link. Therefore, ITW/AA communication link survivability methods can be applied to RPAS. The ITW/AA assumes a defense-in-depth approach to communication link survivability through redundancy, and physical and electronic hardening that should be integrated into RPAS communication structure. Specifically, DOD should continue to invest in RPAS C3 dispersion through programs like OneSystem and BACN to provide redundancy within the system of systems. The DOD should also invest in hardening; physical and electronic hardening of the GCS, and electronic hardening of the communication node and the UAV for a subset of RPAS fielded. Because of CTB Treaty

constraints, investment in subsystem level and/or system level EMP validation testing facilities is required to ensure the live fire survivability of RPAS in an EMP environment. To oversee the system level issues of the "-ilities," including interoperability and survivability, and maintain balance between them across the family of RPAS, the CJCS should designate an RPAS Systems Engineer. A good candidate for the job is the JUAS-COE, which basically already holds the RPAS Systems Engineer job on interoperability for the Joint Staff. Lastly, the DOD should commit to a defense-in-depth survivability policy for RPAS. Rivals can use the threats to RPAS described here to deter US action through an asset hostage deterrent strategy because the threats can produce strategic effects. The likelihood of an adversary adopting this strategy is higher because they could achieve significant tactical and operational effects, particularly as combat RPAS take on a greater percentage of combat missions. Adopting a defense-in-depth survivability approach for RPAS can contribute to an American counter-deterrent strategy of takeback to deal with the strategic vulnerabilities. [102] Should an opponent attack strategic assets, it is unlikely they would be able to consolidate any strategic gains because there would be few if any corresponding tactical or operational advantage attained in the assault. It is crucial to adopt this policy now, because as the example of internet security demonstrates, the US military RPAS capabilities may wind up saddled with vulnerabilities, resulting from prioritizing interoperability too highly over survivability, for a long time to come.

---

1. Joint Chiefs of Staff (JCS), *Joint Acronyms and Abbreviations* (17 March 2009), http://www.dtic.mil/doctrine/jel/doddict/acronym/i/13278.html, (accessed 21 September 2009).

2. Alan D. Zimm, "Deterrence: Basic Theory, Principles, and Implications," *Strategy Review* 25, no. 2 (1997); 45.

3. Ibid., 42.

4. Ibid., 45.

5. Ibid., 42-45.

6. Department of Defense (DOD), *National Defense Strategy* (June 2008), 4.

7. Elizabeth Bone and Christopher Bolkom, *Unmanned Aerial Vehicles: Background and Issues for Congress*, (Congressional Research Service; The Library of Congress, 25 Apr 2003), 1-18.

8. *The Effects of War Casualties on U.S. Public Opinion*, (RAND; Santa Monica, California, June 1994), 2.

9. Department of Defense (DOD), *Unmanned Systems Roadmap 2007 - 2032* (2007), 19.

10. Ibid., 19.

11. Ibid., 3.

12. Office of the Secretary of Defense (OSD), *Unmanned Aerial Vehicles Roadmap 2002 - 2027* (December 2002), iv.

13. Office of the Secretary of Defense (OSD), *Unmanned Aerial Vehicles Roadmap 2000 - 2025* (April 2001), ii.

14. Michael Hoffman, "UAV pilot career field could save $1.5B," *Air Force Times*, 2 March 2009, http://www.airforcetimes.com/news/2009/03/airforce_uav_audit_030109/, (accessed 15 December 2009).

15. Nic Robertson, "How Robot Drones Revolutionized the Face of Warfare," *CNN.com/world*, 26 July 2009, http://www.cnn.com/2009/WORLD/americas/07/23/wus.warfare.remote.uav/index.html, (accessed 22 September 2009).

16. DOD, Unmanned Systems Roadmap, 3.

17. Department of the Air Force, Air Force Handbook: 108th Congress, First Session, 50.

18. Ibid., 50.

19. Laurie Ure, "Armchair pilots striking Afghanistan by remote control," *CNN.com/technology*, 9 July 2008, http://www.cnn.com/2008/TECH/07/09/remote.fighters/index.html, (accessed 21 October 2009).

20. Marine Corps Weapons Procedure (MCWP) 3-42.1, *Unmanned Aerial Vehicle Operations* (August 2003), 1-3.

21. Col Robert B. Giffen, *US Space System Survivability: Strategic Alternatives for the 1990s*, (Washington, DC: National Defense University Press, 1982), 29.

22. "Predator Unmanned Aerial Vehicle (UAV) Ground Control Station (GCS) (United States), Payloads," *Jane's Electronic Mission Aircraft* (15 April 2009), http://www.janes.com/articles/Janes-Electronic-Mission-Aircraft/Predator-Unmanned-Aerial-Vehicle-UAV-Ground-Control-Station-GCS-United-States.html, (accessed 18 October 2009).

23. Ibid.

24. United States Air Force (USAF), *Milstar Satellite Communications System Factsheet* (March 2009), http://www.af.mil/information/factsheets/factsheet.asp?fsID=118, (accessed 22 September 2009).

25. Ibid.

26. Giffen, US Space System Survivability, 30.

27. MCWP 3-42.1, *UAV Operations*, 1-3.

28. Tim Bond, Michael G. Matlock, Thomas Hamilton, Carl Rhodes, Michael Scheiern, David r. Frelinger, and Robert Uy, *Employing Commercial Satellite Communications: Wideband Investment Options for the Department of Defense*, (RAND; Santa Monica, CA, 2000), 72.

29. Curtis Peebles, *High Frontier: The United States Air Force and the Military Space Program* (Washington, DC: Air Force History and Museums Program, 1997), 47.

30. John G. Drew, Russell Shaver, Kristin F. Lynch, Mahyar A. Amouzegar, and Don Snyder, *Unmanned Aerial Vehicle End-to-End Support Considerations*, (RAND; Santa Monica, CA, 2005), 38, 42.

31. Bond, Commercial Communications Satellites, 70.

32. Ibid., 74.

33. MCWP 3-42.1, *UAV Operations*, 1-3.

34. DOD, Unmanned Systems Roadmap, 43.

35. Air Force Instruction (AFI) 11-2MQ-1, *MQ-1 -- Operations Procedures* (29 November 2007), Vol. 3, 8.

36. Air Force Instruction (AFI) 11-2MQ-9, *MQ-9 -- Operations Procedures* (28 November 2008), Vol. 3, 8.

37. Air Force Instruction (AFI) 11-2RQ-4, *RQ-4 -- Operations Procedures* (14 September 2007), Vol. 3, 11-12.

38. National Space-Based Positioning, Navigation, and Timing Coordination Office, *Global Positioning System*, http://www.gps.gov, (accessed 16 December 2009).

39. Federal Aviation Administration, *RVSM Aircraft Certification* (15 April 2004), http://www.faa.gov/about/office_org/field_offices/fsdo/ric/local_more/media/seminars/RVSM%20135%20Seminar.ppt, (accessed 16 December 2009).

40. United States Air Force, *Defense Satellite Communications System Factsheet* (October 2006), http://www.af.mil/information/factsheets/factsheet.asp?fsID=95, (accessed 22 September 2009).

41. Peebles, *High Frontier*, 47.

42. Lt Col Mark Nichols, "Uninhabited Combat Air Vehicles and Commercial Satellites: 'The Missing Link'," (Maxwell AFB, AL: Air War College, April 1998), 25.

43. Kelly Young, "Anti-Satellite Test Generates Dangerous Space Debris," *New Scientist*, 20 January 2007, http://space.newscientist.com/article.ns?id=dn10999 (accessed 1 November 2008), in Lt Col James Mackey, "Recent US and Chinese Antisatellite Activities," *Air & Space Power Journal* 23, no.3 (Fall 2009); 84-85.

44. Lt Col Clayton K. S. Chun, "Shooting Down a 'Star': Program 437, the US Nuclear ASAT System and Present-Day Copycat Killers," CADRE no. 6, (Air University Press; Maxwell AFB, AL, April 2000), 36.

45. Young, "Anti-Satellite Test."

46. Los Angeles Air Force Base (LAAFB), *Global Positioning System Fact Sheet* (August 2009), http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5325, (accessed 21 October 2009).

47. Joint Publication (JP) 3-01.5, *Doctrine for Joint Theater Missile Defense* (22 February 1996), viii.

48. Department of Defense (DOD), *Military Critical Technologies List Section 20: Weapons Effects Technology* (Office of the Under Secretary of Defense Acquisition, Technology, and Logistics, February 2008), 20.1-20.14.

49. Giffen, US Space System Survivability, 30.

50. Chun, "Shooting Down a 'Star'," 21.

51. Dr. John S. Foster, Jr., Earl Gjelde, Dr. William R. Graham, Dr. Robert J. Herman, Henry J. Kluepfel, Gen Richard L. Lawson, Dr. Graham K. Soper, Dr. Lowell L. Wood, Jr., Dr. Joan B. Woodard, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures*, (Electromagnetic Pulse Commission; Mclean, VA, April 2008), 164-166.

52. Foster, *EMP Attack*, 165-166.

53. Hon. Donald H. Rumsfeld, et. al., *Report to the Commission to Assess United States National Security Space Organization and Management* (11 January 2001), 21, http://space.au.af.mil/space_commission/Space Commission Threats, (accessed 19 October 2009).

54. LAAFB, GPS Fact Sheet.

55. Foster, *EMP Attack*, vi.

56. Lt Col Jeffrey T. Butler, "The Influence of Politics, Technology, and Asia on the Future of US Missile Defense," Walker Paper no. 7 (Maxwell AFB, AL: College of Aerospace Doctrine, Research, and Education, 2007), 7.

57. Jacques S. Gansler, Hans Binnendijk, John M. Borky, "Information Assurance: Trends in Vulnerabilities, Threats, and Technologies," (Washington, DC: National Defense University Center for Technology and National Security Policy, January 2004), 54.

58. Lecturer, "Moral Ideas about War: Just War Theory," (lecture, Air Command and Staff College, Maxwell AFB, AL, 24 October 2009).

59. LTC Kenneth F. McKenzie, Jr., "Revenge of the Melians: Asymmetric Threats and the Next QDR," McNair Paper no. 62 (Washington, DC: Institute for National Strategic Studies, National Defense University, 2000), 34-39.

60. USAF, *Milstar*.

61. Giffen, US Space System Survivability, 36-37.

62. DOD, Unmanned Systems Roadmap, 54.

63. OSD, *UAV Roadmap 2000*, 22-23.

64. OSD, UAV Roadmap 2002, 31.

65. DOD, Unmanned Systems Roadmap, 12, 27, 117.

66. Ibid., iii-v.

67. OSD, UAV Roadmap 2000.

68. OSD, UAV Roadmap 2002.

69. DOD, Unmanned Systems Roadmap, 13-19, 54.

70. Ibid., 13.

71. Vinton Cerf, "Future of Cyberspace," (lecture, Air Force Association Air & Space Conference, National Harbor, MD, 14 September 2009).

72. Ibid.

73. OSD, *UAV Roadmap 2000*, 22-23.

74. OSD, UAV Roadmap 2002, 31.

75. DOD, Unmanned Systems Roadmap, 11-12.

76. Ibid., 12, 29.

77. Ibid., 7.

78. Ibid., 7.

79. DOD Directive (DODD) 8500.1, *Information Assurance* (21 November 2003).

80. DOD, *Unmanned Systems Roadmap*, 11-19, 25-42.

81. Ibid., 53, 118-119.

82. Systems Engineering Department, "Departmental Statement on Systems Engineering Scholarship," (Naval Postgraduate School, Monterrey, CA, August 2004), http://www.nps.edu/Academics/Schools/GSEAS/Departments/SE/Documents/SE-Scholarship.doc, (accessed 13 December 2009), 1.

83. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5119.01C, Charter for the Centralized Direction, Management, Operation, and Techincal Support of the Nuclear Command, Control, and Communication System (14 December 2007), A-2.

84. DOD, Unmanned Systems Roadmap, 12, 29.

85. CJCSI 5119.01C, Nuclear Command, Control, and Communication, A-2.

86. DOD, Unmanned Systems Roadmap, 13.

87. Ibid., 50.

88. Nichols, "UCAVs," 25-26.

89. Bond, Commercial Communications Satellites, 75-76.

90. Stephen Trimble, "Seamless airborne networks are becoming a reality thanks to bridging technology," *Jane's Defence Weekly*, 24 January 2007, http://integrator.hanscom.af.mil/2007/January/01252007/01252007-15.htm, (accessed 17 October 2009).

91. Cerf, "Future of Cyberspace."

92. International Space Station Program Scientist's Office, *Delay Tolerant Networking Fact Sheet* (15 May 2009), http://www.nasa.gov/mission_pages/station/science/experiments/DTN.html, (accessed 16 October 2009).

93. Defense Advanced Research Projects Agency, *Disruption Tolerant Networking (DTN)*, http://www.darpa.mil/sto/strategic/dtn.html, (accessed 16 October 2009).

94. McKenzie, "Revenge of the Melians," 35.

95. Noah Schachtman, "Iran's 'Space Missile?' Yawn, It's a SCUD," *Wired.com*, 26 February 2007, http://www.wired.com/dangerroom/2007/02/irans_new_space/, (accessed 13 December 2009).

96. Florios Bardanis, "Kill Vehicle Effectiveness for Boost Phase Interception of Ballistic Missiles," (MS thesis, Naval Postgraduate School, June 2004), 5-6.

97. Foster, *EMP Attack*, 164-166.

98. CJCSI 5119.01C, Nuclear Command, Control, and Communication, A-2.

99. Ibid., A-2 - A-3.

100. DOD, Unmanned Systems Roadmap, 29.

101. Zimm, "Deterrence," 45.

102. Ibid., 45.

Bibliography

Air Force Instruction (AFI) 11-2MQ-1. *MQ-1 -- Operations Procedures*, 29 November 2007. Vol. 3.

Air Force Instruction (AFI) 11-2MQ-9. *MQ-9 -- Operations Procedures*, 28 November 2008. Vol. 3.

Air Force Instruction (AFI) 11-2RQ-4. *RQ-4 -- Operations Procedures*, 14 September 2007. Vol. 3.

Bardanis, Florios. "Kill Vehicle Effectiveness for Boost Phase Interception of Ballistic Missiles." MS thesis, Naval Postgraduate School, June 2004.

Bond, Tim, Michael G. Matlock, Thomas Hamilton, Carl Rhodes, Michael Scheiern, David r. Frelinger, and Robert Uy. *Employing Commercial Satellite Communications: Wideband Investment Options for the Department of Defense*. RAND; Santa Monica, CA, 2000.

Bone, Elizabeth and Christopher Bolkom. *Unmanned Aerial Vehicles: Background and Issues for Congress*. Congressional Research Service; The Library of Congress, 25 Apr 2003.

Butler, Lt Col Jeffrey T. "The Influence of Politics, Technology, and Asia on the Future of US Missile Defense." Walker Paper no. 7. Maxwell AFB, AL: College of Aerospace Doctrine, Research, and Education, 2007.

Cerf, Dr. Vinton. "Future of Cyberspace." Lecture. Air Force Association Air & Space Conference, National Harbor, MD, 14 September 2009.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5119.01C. Charter for the Centralized Direction, Management, Operation, and Techincal Support of the Nuclear Command, Control, and Communication System, 14 December 2007.

Chun, Lt Col Clayton K. S. "Shooting Down a 'Star': Program 437, the US Nuclear ASAT System and Present-Day Copycat Killers." CADRE no. 6. Air University Press; Maxwell AFB, AL, April 2000.

Defense Advanced Research Projects Agency. *Disruption Tolerant Networking (DTN)*. http://www.darpa.mil/sto/strategic/dtn.html, (accessed 16 October 2009).

Department of the Air Force (DAF). Air Force Handbook: 108th Congress, First Session.

Department of Defense (DOD). *Military Critical Technologies List Section 20: Weapons Effects Technology*. Office of the Under Secretary of Defense Acquisition, Technology, and Logistics, February 2008.

Department of Defense (DOD). *Unmanned Systems Roadmap 2007 - 2032*, 2007.

Department of Defense (DOD), *National Defense Strategy*, June 2008.

Department of Defense (DOD) Directive 8500.1. *Information Assurance*, 21 November 2003.

Drew, John G., Russell Shaver, Kristin F. Lynch, Mahyar A. Amouzegar, and Don Snyder. *Unmanned Aerial Vehicle End-to-End Support Considerations*. RAND; Santa Monica, CA, 2005.

The Effects of War Casualties on U.S. Public Opinion. RAND; Santa Monica, California, June 1994.

Federal Aviation Administration (FAA). *RVSM Aircraft Certification*. 15 April 2004. http://www.faa.gov/about/office_org/field_offices/fsdo/ric/local_more/media/seminars/RVSM%20135%20Seminar.ppt, (accessed 16 December 2009).

Foster, Dr. John S. Jr., Earl Gjelde, Dr. William R. Graham, Dr. Robert J. Herman, Henry J. Kluepfel, Gen Richard L. Lawson, Dr. Graham K. Soper, Dr. Lowell L. Wood, Jr., Dr. Joan B. Woodard. *Report of the Commission to Assess the Threat to the United States from*

Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures. Electromagnetic Pulse Commission; Mclean, VA, April 2008.

Gansler, Jacques S., Hans Binnendijk, John M. Borky. "Information Assurance: Trends in Vulnerabilities, Threats, and Technologies." Washington, DC: National Defense University Center for Technology and National Security Policy, January 2004.

Giffen, Col Robert B. *US Space System Survivability: Strategic Alternatives for the 1990s*. Washington, DC: National Defense University Press, 1982.

Hoffman, Michael. "UAV pilot career field could save $1.5B." *Air Force Times*, 2 March 2009. http://www.airforcetimes.com/news/2009/03/airforce_uav_audit_030109/, (accessed 15 December 2009).

International Space Station Program Scientist's Office. *Delay Tolerant Networking Fact Sheet.* 15 May 2009. http://www.nasa.gov/mission_pages/station/science/experiments/DTN.html, (accessed 16 October 2009).

Joint Chiefs of Staff (JCS). *Joint Acronyms and Abbreviations*, 17 March 2009. http://www.dtic.mil/doctrine/jel/doddict/acronym/i/13278.html, (accessed 21 September 2009).

Joint Publication (JP) 3-01.5. *Doctrine for Joint Theater Missile Defense*, 22 February 1996.

Los Angeles Air Force Base (LAAFB). *Global Positioning System Fact Sheet*, August 2009. http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5325, (accessed 21 October 2009).

Lecturer. “Moral Ideas about War: Just War Theory.” Lecture. Air Command and Staff College, Maxwell AFB, AL, 24 October 2009.

Marine Corps Weapons Procedure (MCWP) 3-42.1. *Unmanned Aerial Vehicle Operations*, August 2003.

McKenzie, LTC Kenneth F., Jr. “Revenge of the Melians: Asymmetric Threats and the Next QDR.” McNair Paper no. 62. Washington, DC: Institute for National Strategic Studies, National Defense University, 2000.

National Space-Based Positioning, Navigation, and Timing Coordination Office. *Global Positioning System*. http://www.gps.gov, (accessed 16 December 2009).

Nichols, Lt Col Mark. “Uninhabited Combat Air Vehicles and Commercial Satellites: ‘The Missing Link’.” Maxwell AFB, AL: Air War College, April 1998.

Office of the Secretary of Defense (OSD). *Unmanned Aerial Vehicles Roadmap 2000 - 2025*, April 2001.

Office of the Secretary of Defense (OSD). *Unmanned Aerial Vehicles Roadmap 2002 - 2027*, December 2002.

Peebles, Curtis. *High Frontier: The United States Air Force and the Military Space Program*. Washington, DC: Air Force History and Museums Program, 1997.

“Predator Unmanned Aerial Vehicle (UAV) Ground Control Station (GCS) (United States), Payloads.” *Jane’s Electronic Mission Aircraft*, 15 April 2009. http://www.janes.com/articles/Janes-Electronic-Mission-Aircraft/Predator-Unmanned-Aerial-Vehicle-UAV-Ground-Control-Station-GCS-United-States.html, (accessed 18 October 2009).

Robertson, Nic. “How Robot Drones Revolutionized the Face of Warfare” *CNN.com/world*, 26 July 2009. http://www.cnn.com/2009/WORLD/americas/07/23/wus.warfare.remote.uav/index.html, (accessed 22 September 2009).

Rumsfeld, Hon. Donald H., et. al. *Report to the Commission to Assess United States National Security Space Organization and Management.* 11 January 2001. http://space.au.af.mil/space_commission/Space Commission Threats, (accessed 19 October 2009).

Schachtman, Noah. “Iran’s ‘Space Missile?’ Yawn, It’s a SCUD.” *Wired.com*, 26 February 2007. http://www.wired.com/dangerroom/2007/02/irans_new_space/ (accessed 13 December 2009).

Systems Engineering Department. “Departmental Statement on Systems Engineering Scholarship.” Naval Postgraduate School, Monterrey, CA, August 2004. http://www.nps.edu/Academics/Schools/GSEAS/Departments/SE/Documents/SE-Scholarship.doc, (accessed 13 December 2009).

Trimble, Stephen. “Seamless airborne networks are becoming a reality thanks to bridging technology.” *Jane’s Defence Weekly*, 24 January 2007. http://integrator.hanscom.af.mil/2007/January/01252007/01252007-15.htm, (accessed 17 October 2009).

United States Air Force (USAF). *Defense Satellite Communications System Factsheet*, October 2006. http://www.af.mil/information/factsheets/factsheet.asp?fsID=95, (accessed 22 September 2009).

United States Air Force (USAF). *Milstar Satellite Communications System Factsheet*, March 2009. http://www.af.mil/information/factsheets/factsheet.asp?fsID=118, (accessed 22 September 2009).

Ure, Laurie. "Armchair pilots striking Afghanistan by remote control." *CNN.com/technology*, 9 July 2008. http://www.cnn.com/2008/TECH/07/09/remote.fighters/index.html, (accessed 21 October 2009).

Young, Kelly. "Anti-Satellite Test Generates Dangerous Space Debris." *New Scientist*, 20 January 2007. http://space.newscientist.com/article.ns?id=dn10999 (accessed 1 November 2008).

in Lt Col James Mackey. "Recent US and Chinese Antisatellite Activities." *Air & Space Power Journal* 23, no.3 (Fall 2009): 82-93.

Zimm, Alan D. "Deterrence: Basic Theory, Principles, and Implications." *Strategy Review* 25, no. 2 (1997); 42-50.